

			-	- 05 001 11 505	T ATTORNEY DO	CKET NO	S	heet	1 of 1
ORM PTO-1	449			T OF COMMERCE DEMARK OFFICE	1573.101	0	1	0/028	
LIST OF	REF	ERENCES C	ITED BY	APPLICANT	FIRST NAMED  Koichi IT				
	(Us	e several sheets	if necessar	· ·v)	FILING DATE	00.000		ROUP AR	TINIT
				•	Decembe	er 28, 2001	1 2	131	
			U.S. PA	ATENT DOCUME	NTS	_			
EXAMINER INITIAL		DOCUMENT NO.	DATE	NAME		CLASS	SU CLA		FILING DATE
TMS	AA	5,452,358	09/1995	Normile et al.			1		
	AB					RE	CEIV	ED	
	AC					AU	G 1 4 2	003	
	AD					Technol	ogy Cent	er 210	0
<del></del>	AE								
	AF								
T.M (	AG	NO. 0 981 223 A2	DATE 02/2000	COUNTR European Paten		CLASS	CLASS	YE	S NO
7:M(	AG	0 981 223 A2 0 792 041 A2	02/2000	European Paten  European Paten				<del> </del>	
(100)	Al	013204172	00/100/	- Caropauri atan				-	
	AJ			<del>                                     </del>					
	AK							-	
	AL							-	
	A.			<u> </u>					
THER RE	FERE	NCES (Including	Author, T	itle, Date, Pertine	nt Pages,	Etc.)			NSLATIC ES NO
TMS	AM	Analysis Attack	ks", PROCE	Securing the AES EEDINGS OF FAS OP 2000, April 10	T SOFTWA	RE			
XAMINER	7,	A. S.	r 1	DATE	CONSIDER	RED	•		
. 1			_////	_   / 0	- / / /	لسارك			

),C	IPE
FEB	0 1 2002 8
THE STATE OF THE S	

ORM PTO-1449 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY DOCKET NO.

Sheet 1 of 2

1573.1010 FIRST NAMED INVENTOR

10/028,265

LIST OF REFERENCES CITED BY APPLICANT

Koichi ITO, et al.

FILING DATE

GROUP ART UNIT

(Use several sheets if necessary)

December 28, 2001

U.S. PATENT DOCUMENTS

			0.0.17	I EITI OOOOMEITIO			
*EXAMINER INITIAL		DOCUMENT NO.	DATE	NAME	CLASS	SUB- CLASS	FILING DATE
	AA						
	AB						
	AC						

**FOREIGN PATENT DOCUMENTS** 

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUB- CLASS	TRANSL YES	ATION NO
TMS	AD	2000-305453	11/2000	Japan			Х	
	AE	WO 99/67919	12/1999	WIPO	<u> </u>	-	Х	
	AF	WO 00/46953	08/2000	WIPO	_	•	Х	
	AG	WO 00/27068	05/2000	WIPO			Х	
	AH	WO 00/49765	08/2000	WIPO		-	Х	
	Al	WO 01/10077.	02/2001	WIPO		)	Х	

OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, Etc.)

PM	SAJ	Kocker, Paul, et al., "Differential Power Analysis" in <u>Proceedings of Advances in Cryptology-CRYPTO '99</u> , Springer-Verlag 1999. pages 388-397.
	<u> </u>	
1	AK	Messerges, Thomas, et al., "Power Analysis Attacks of Modular Exponentiation in
		Smartcards", Cryptographic Hardware and Embedded Systems (CHES '99), Springer-
1 1		Verlag, pages 144-157
	AL	Akkar, Mehdi-Laurent, et al., "Power Analysis, What is Now Possible", ASIACRYPT 2000, Pages 489-502.
	AM	Messerges, Thomas S., "Securing the AES Finalists Against Power Analysis Attacks", <u>Proceedings of Fast Software Encryption Workshop 2000</u> , Springer-Verlag, April 2000, which is called "a masking method."

Shukaya DATE CONSIDERED 10/4/05

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Sheet 2 of 2

FORM PTO-1449

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY DOCKET NO. 1573.1010 APPLICATION NO. 10/028,265
FIRST NAMED INVENTOR

LIST OF REFERENCES CITED BY APPLICANT

FEB 0 1 2002

(Use several sheets if necessary)

Koichi ITO, et al.

FILING DATE
December 28, 2001

GROUP ART UNIT

## **U.S. PATENT DOCUMENTS**

*EXAMINER INITIAL		DOCUMENT NO.	DATE	NAME	CLASS	SUB- CLASS	FILING DATE
	ВА						
	ВВ						
	ВС						
	BD						
	BE		·				
	BF						

FOREIGN PATENT DOCUMENTS

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUB- CLASS	TRANSLAT YES N	ION IO
1 Ms	BG	WO 00/24155	04/2000	WIPO	-	1.	Х	
1m5	вн	WO 00/24156	04/2000	WIPO	<u> </u>		X	
	ВІ							
	BJ			·	<u> </u>			
	вк							
	BL ·							

OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, Etc.)

			THEN REPERENCES (Including Addition, Time, Date, 1 Chancing ages, Etc.)
1	145	вм	Messerges, Thomas S. et al., "Investigations of Power Analysis Attacks on Smartcards", Proceedings of USENIX Workshop on Smartcard Technology, March 1999.
		BN	Chari, Suresh, et al., "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards", Second Advanced Encryption Standard Candidate Conference, March 1999.
		80	FIPS 46, "Data Encryption Standard" Federal Information Processing Standards Publication 46, U.S. Departement of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, VA, 1977.
	<i>y</i>	ВР	http://csrc.nist.gove/encryption/aes/rijndael/Rijndael.pdf (which is linked from http://www.nist.gov/aes/).

EXAMINER MINISTER STATE OF THE	DATE CONSIDERED	10/4/05
*EXAMINER: Initial if reference considered, whether of not citation	is in conformance with MPEP 6	09: Draw line through citation if